REMARKS

Claims 1-4 are pending. The office action rejects claims 1-4.

Claim 1 is amended to claim a method for encrypting data.

Claims 1 and 4 are amended to eliminate the "consisting" language that the Examiner objected to in the Office Action.

Claims 1 and 4 are also amended to claim that the encryption of the first symmetric key produces an "encrypted first symmetric key". This is to help clarify what the invention claims in these respective claims.

Claim 3 is amended to eliminate "encryption" as being the type of function used.

No new matter was entered in view of these amendments.

Rejection of Claims 1-4 under 35 U.S.C. 112, Second Paragraph

The Examiner rejected Claims 1-4 under 35 U.S.C. 112, Second Paragraph as being indefinite for several reasons listed below with the Applicants' remarks.

A. The Examiner objected to the claims as to recite that it is unclear as to which key "a symmetric key" refers to, when there is recitation of a first key, second key, or a new key. Applicants have eliminated this phrase from the preamble of the method. The method now recites "Method for encrypting data", which should overcome this rejection.

B. The Examiner objected to the phrase "method comprising the steps that consist" in Claims 1 and 4 as containing both an open ended clause (comprising) and a closed ended clause (consisting). Claim 1 is amended to recite "the method comprising the steps for the device of a first type of" which eliminates this inconsistent language.

C. The Examiner rejected Claim 3 as claiming implying that function that was reversible, even though the function from Claim 2 is a "one way" function. Clearly, the idea of a hash function does not have to be reversible, so the amendment to Claim 3 should overcome the Examiner's rejections.

D. If the Examiner is still of the opinion that these claims are still to be rejected under 35 U.S.C. 112, Second Paragraph, the Applicants respectfully request that the Examiner discuss such issues with the Applicants by telephone.

Rejection of Claims 1-4 under 35 U.S.C. 103(a)

The Office action rejects claims 1, 2, and 4 under 35 U.S.C. 103(a) over Menezes et al. ("Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, FL CRC Press, US. 1997, pgs. 497-553, hereafter referred to as 'Menezes') in view of Patel et al. (U.S. Publication 2005/0025091, hereafter referred to as 'Patel'). Reconsideration is respectfully requested in view of the following comments.

Applicants' claim 1 includes in part the features of:

"*an encrypted first symmetric key which is generated from the encryption of said first symmetric key with a second symmetric network key known only by at least one device of a second type connected to said network*".

The Office Action on page 4 states that such a feature is known in the Menezes reference, "said first symmetric key encrypted with a second symmetric network key known only by a least one device of said second type connected to said network [session key encrypted by key K; pg. 497]." This is not correct because on page 497 of the Menezes reference (with Patel) there is a disclosure that, "Point-to-point key update techniques based on symmetric encryption make use of long term symmetric key K *shared a priori by two parties A and B*," (emphasis added). This disclosure of Menezes in view of Patel suggests that the key "K" disclosed in the reference (as the Examiner's second key) is known by the first device and the second device. Clearly, this is not the case with the claimed invention of Claim 1.

Claim 1 recites that the second key is "*a second symmetric network key known only by at least one device of a second type*" where the second device type is different from said first device type. That is, Claim 1 claim that the key the Examiner's "second key" is only present in the second device type, not the first device type. The Menezes reference, in view of the Examiner's recitation and Patel, discloses that the second key is known by both device types; this is different than what is claimed in Claim 1.

Claim 1 claims that the first type of device contains an encrypted first key that was encrypted by a second key, where this second key is present only in the second type of device. The first type of device does not know anything about the second key. Hence, attributes of the second type of device for encryption are preserved because the first type of device will not know about the second key which the second type of device contains. These features of Claim 1 are neither disclosed nor suggested in Menezes and Patel, alone or in combination.

Claim 1 is patentable for the reasons given above. In addition, Claims 2-4 are patentable as such claims depend on allowable Claim 1.

CONCLUSION

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6809, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
A. Durand et al.

By: Joel M. Fogelson
Attorney for Applicants
Registration No. 43,613

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: November 9, 2009